

User's Guide for Aiko SecuWipe

SecuWipe

Data wiping software
for
Windows Mobile
touch-screen phones

Version 1.1

Secure data wiping software for:

- Windows Mobile 6.0, 6.1, 6.5 Professional
- Windows Mobile 6.0, 6.1, 6.5 Classic
- Windows Mobile 5.0 for Pocket PC Phone Edition
- Windows Mobile 5.0 for Pocket PC
- Windows Mobile 2002/2003/2003SE/2005
- Windows CE 3.0/4.0/4.1/4.2/5.0/5.2/6.x
- Handheld PC 2000 (Windows CE 3.0)
- Pocket PC /2002/2003/Phone Edition

© Aiko Solutions. All rights reserved.
[869 High Road, London, N12 8QA, United Kingdom](http://www.aikosolutions.com)
<http://www.aikosolutions.com>
info@aikosolutions.com



Contents

[User's Guide for Aiko SecuWipe](#)

[Definitions](#)

[Overview](#)

[Data Sanitizing Methods](#)

[Platform and System Requirements](#)

[Installing and Upgrading](#)

[Installing](#)

[Uninstalling](#)

[Upgrading](#)

[Using SecuWipe](#)

[Wipe File](#)

[Wipe Folder](#)

[Wipe Free Space](#)

[Custom Wipe](#)

[Wipe Scheduler](#)

[Time-based Schedule](#)

[Upon Soft Reset](#)

[Upon SMS](#)

[Upon SIM](#)

[Settings](#)

[Enable System Tray Icon](#)

[Enable Exit Confirmation](#)

[Minimize to Tray on Close](#)

[Check for Updates](#)

[Autorun at Startup](#)

[Enable Error Logging](#)

[Exiting SecuWipe](#)

[Command line support](#)

[Command Line Usage Examples](#)

[Performance - Wipe Speeds](#)

[Recommended Procedures](#)

[How to Register](#)

[Contacts](#)

Definitions

Definitions. In this User's Guide the following definitions are being used, singular as well as plural.

1.1 Windows Mobile phone, Windows Phone, Windows Mobile touch-screen phone, PDA, handheld: personal digital assistant, a handheld device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer. It generally includes at least a name and address database, to-do list and note taker. PDAs may be combined with cellphones and other wireless technologies, providing a mobile office for people on the go. PDAs are pen based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard which is tapped with the pen. Data are synchronized between the PDA and desktop computer via cable or wireless transmission.

1.2 Smartphone: a category of mobile device that provides advanced capabilities beyond a typical mobile phone. Smartphones run complete operating system software that provides a standardized interface and platform for application developers. By the strict definition, smartphones are distinct from

PDA-based devices running operating systems such as Palm OS or Windows Mobile for Pocket PCs. While PDA-based devices usually have a touch-screen for pen input, smartphones usually have a standard phone keypad for input. The major smartphone environments are Symbian, Blackberry, Palm and Windows Mobile. Microsoft branded the term "Smartphone" (capital S) within its Windows Mobile platform.

1.3 Software: the software distributed by Aiko Solutions and Documentation, as well as any future programming fixes, updates and upgrades thereof.

1.4 You: you, the end user of the Software, also used in the form "Your" where applicable.

1.5 Documentation: Aiko Solutions grants you a non-exclusive license to use the Documentation in connection with your use of the Software. You may not distribute the Documentation without providing references to Aiko Solutions company and Aiko Solutions website (<http://www.aikosolutions.com/>).

All right, title and interest (including but not limited to copyright, patent, trade secret and all other intellectual property and proprietary rights worldwide) in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software are owned by Aiko Solutions and its suppliers. You shall not remove, cover or alter any of Aiko Solutions' (or its designated suppliers') copyright, trademark or other proprietary notices placed upon, embedded in or displayed by the Software or on its packaging and related materials.

No Warranties. The Software is being delivered to you "AS IS" and Aiko Solutions makes no warranty as to its use or performance. AIKO SOLUTIONS AND ITS SUPPLIERS DO NOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE. YOU ASSUME THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE OF THE SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AIKO SOLUTIONS AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, TERMS, AND CONDITIONS, EITHER EXPRESS OR IMPLIED, BY STATUTE, COMMON LAW OR OTHERWISE, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES, TERMS, AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT WITH REGARD TO THE SOFTWARE, ITS SATISFACTORY QUALITY, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES.

Limitation of Liability. TO THE MAXIMUM EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL AIKO SOLUTIONS BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE SOFTWARE, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF AIKO SOLUTIONS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

Aiko Solutions can not be held responsible nor render any assistance in the event you accidentally erase important data or do not perform backups.

Back to: Contents

Overview

SecuWipe is an advanced data sanitizing (wiping) software for Windows Mobile touch-screen phones

and Windows CE handheld devices.

The program irretrievably deletes sensitive data from your mobile device by overwriting it in accordance with strong data sanitizing methods.

When you delete a file in a usual way, the file is in fact not deleted at all. Usually, all that happens is that the file's name is removed from the file systems' index and the space occupied by the file is marked as available for new data. However, as long as no new data is written on those locations, the 'deleted' file can still be recovered.

Data sanitizing is the only secure way to remove traces of any strictly confidential and highly sensitive data. Files thought to have been deleted contain personal details, bank account details, credit card numbers, etc., can be recovered too easily, and simply hard resetting the device or formatting the removable card is not an effective means of rendering this data inaccessible. If you are going to sell or donate your PDA, data wiping is the only way to ensure you permanently erase all sensitive data, including files, folders, entire removable media cards, as well as all email, contacts, appointments and tasks' databases.

REMEMBER TO BACK UP ANY FILES YOU WANT TO KEEP BEFORE WIPING THE DEVICE.

Data Sanitizing Methods

SecuWipe uses the following data sanitizing methods:

1. Zeroing-out - everything is overwritten with "0" pattern - 1 pass;
2. US Department of Defense - U.S. DoD 5220.22-M (C) - everything is overwritten with a random byte - 1 pass;
3. U.S. DoD 5220.22-M (E) - everything is overwritten with "0", "1" and with a random byte - 3 passes;
4. U.S. DoD 5220.22-M (ECE) - used method #3, then #2, then #3 - 7 passes. PDAs containing top secret data are not permitted to be sanitized by any of DoD5220.22; they must be physically destroyed.
5. Bruce Schneier's algorithm - the first pass overwrites the file with the bit pattern "0", the second with "1", and the next five with a cryptographically random bit pattern (SHA 512-bit is used to generate cryptographic random) - 7 passes.
6. Peter Gutmann's algorithm - 35 overwrite passes in total, it is considered the strongest method for data destruction. This method is, however, time-consuming, wiping a device using Peter Gutmann's method will take more than 5 times longer than wiping the same device with Bruce Schneier's algorithm.

Back to: Contents

Platform and System Requirements

SecuWipe gives you peace of mind when you are selling or donating your Windows phone or Pocket PC. It is also the only way to securely delete all previously "deleted" data to ensure all confidential data will not be recovered by third parties.

SecuWipe currently supports the following PDA platforms:

- Windows Mobile 6/6.1/6.5 Professional
- Windows Mobile 6/6.1/6.5 Classic
- Windows Mobile 5.0 for Pocket PC Phone Edition
- Windows Mobile 5.0 for Pocket PC
- Windows Mobile 2002/2003/2003SE/2005
- Windows CE 3.0/4.0/4.1/4.2/5.0/5.2/6.x
- Handheld PC 2000 (Windows CE 3.0)
- Pocket PC 2002/2003/Phone Edition

System Requirements:

- Low processor speed required: 150 MHz (>250MHz recommended)
- Processor Type: ARM, SH3, SH4, MIPS
- Available Storage Space needed: > 1.8 Mb on computer hard drive, >900Kb on Pocket PC
- ActiveSync: 3.5 or newer for the software installation.

Back to: Contents

Installing and Upgrading

Installing

To install, download SecuWipe desktop installation file (secuwipe.exe) from www.aikosolutions.com/download/, run secuwipe.exe and follow the instructions. In order to be able to install the software, you must accept the End-User License Agreement. Once the installation is complete you may use SecuWipe to sanitize data.

You may also download SecuWipe from your Windows Mobile phone directly. Go to www.aikosolutions.com/download/ and select secuwipe.arm.cab, secuwipe.mips.cab, secuwipe.sh3.cab, secuwipe.sh4.cab or secuwipe.x86.cab depending on the type of your processor. Install this file on your device.

Uninstalling

To uninstall SecuWipe, go to the Settings window on your Pocket PC (Start->Settings). Then choose System-tab->Remove Programs. Choose Aiko SecuWipe program and proceed to Remove.

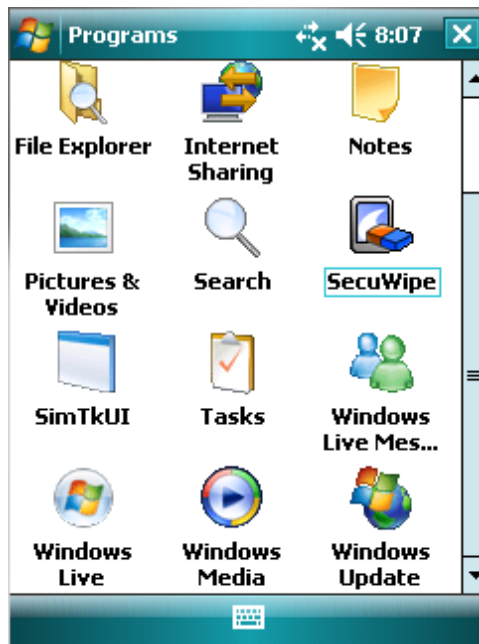
Upgrading

To upgrade to a newer version of SecuWipe you only have to install the newer version over the older one. If a software update completely replaces (full install) a previously licensed version of the software, you may not use both versions of the SecuWipe at the same time nor may you transfer them separately. You may not, not even in parts, circulate the license keys transmitted to you to any third party. You shall keep secret all license keys communicated to you by Aiko Solutions or Aiko Solutions authorized distributors. You are fully liable for damages resulting from unauthorized circulation or distribution. Aiko Solutions reserves the right to block license keys that have not been paid for by the user in due time or the license keys which were delivered to you after transaction which further resulted in a refund or chargeback. Aiko Solutions reserves the right to block illegally distributed license keys as well as to file the suit against the party distributing the keys without permission from Aiko Solutions.

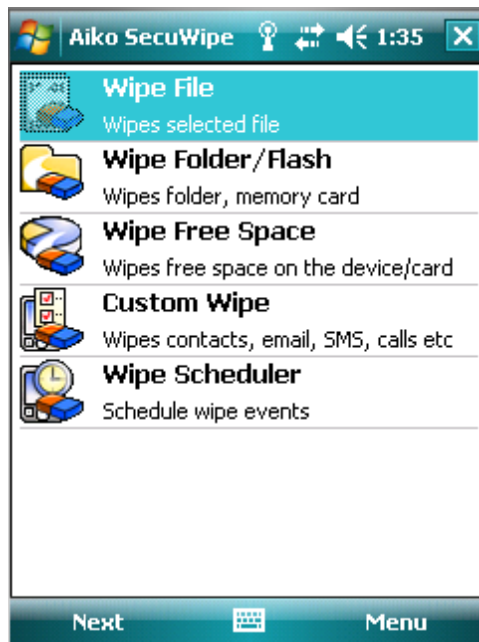
Back to: Contents

Using SecuWipe

Go to Start->Programs and run Aiko SecuWipe.

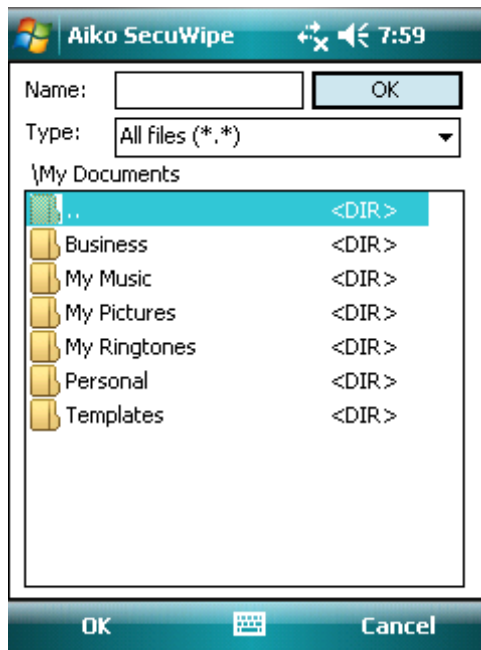


SecuWipe window will appear.

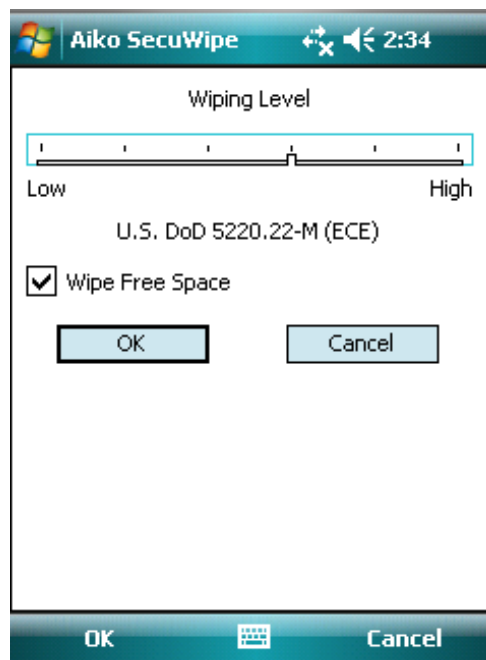


Wipe File

To erase a file, tap Wipe File in Aiko SecuWipe main window.



Browse to the file you intend to erase and select it. The Wiping Level window will open. Here you may select different wiping levels (See [Data Sanitizing Methods](#) for more information).

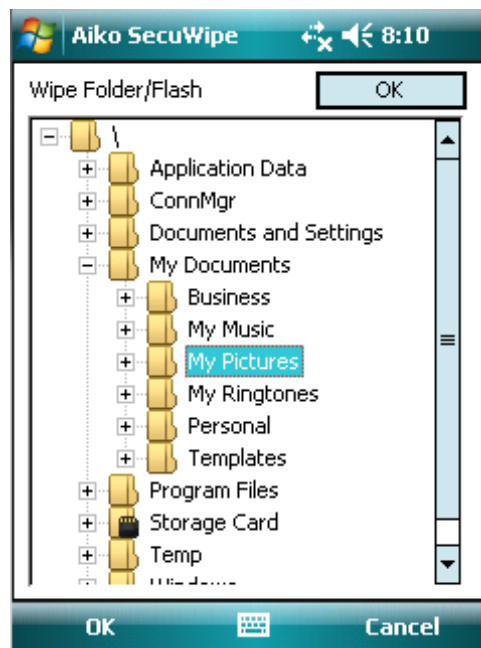


SecuWipe offers the option of wiping the free space (see [Wipe Free Space](#) for more information). It will wipe either the device internal memory or the storage card, depending on location of the file/folder you have selected to wipe. The reason SecuWipe offers you to wipe free space is that when Windows Mobile or Pocket PC applications work with the file, multiple copies of that file can be stored by these applications or Windows may optimize file positioning, making different copies of the file – changing only its address in FAT table. If you wipe the file only without wiping free space there is a big chance that there are portions of this file remaining on the device or its memory card.

Back to: Contents

Wipe Folder

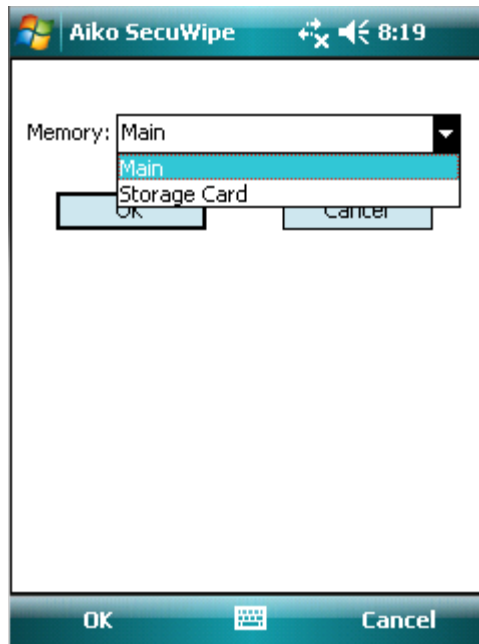
To erase folder, tap Wipe Folder in the SecuWipe window. Locate the folder you intend to wipe and then select data sanitizing algorithm. This will wipe the folder, its subfolders and files.



Back to: Contents

Wipe Free Space

To wipe free space of either the device internal memory or on the removable media cards, tap Wipe Free Space in the SecuWipe window.



The Wipe Free Space is intended to irretrievably delete data in the following cases:

- **To wipe previously deleted files.** If you have previously deleted sensitive files, they may still exist in the free space of your device. Wiping free space will totally eliminate all traces of these files.
- **To wipe temporary files.** When you edit your documents, some programs (such as MS Office) create temporary files, which contain your sensitive information. These temporary files are intermediary copies of your document, and after you finish editing it, these copies are left in the device or memory card free space. Even after you have wiped your initial document, there may exist several copies or parts of these files on your device or storage card. The solution to this is to periodically wipe device free space.

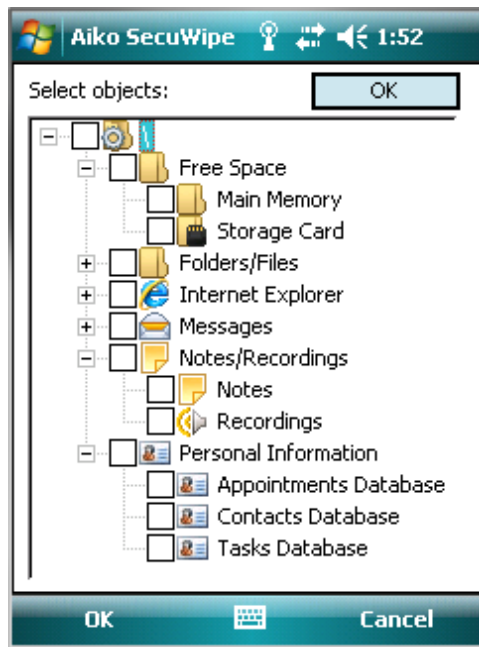
Note: If you wipe the free space on a device by mistake, don't panic. Using this procedure will only wipe your free space, not your data.

Back to: Contents

Custom Wipe

Custom Wipe allows you to delete all data on your Windows phone including:

- Contacts, Calls
- Email, SMS, MMS messages
- Notes, Recordings
- Appointments, Tasks
- Internet Explorer Cache, Cookies, History
- Free Space
- SD card(s)
- Files and Folders



Back to: Contents

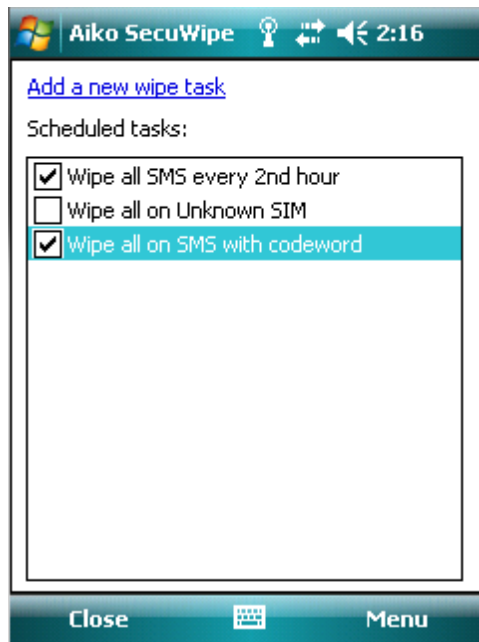
Wipe Scheduler

Wipe Scheduler allows to configure SecuWipe to run wiping tasks automatically. You choose the objects to be wiped in the same way you do it via Custom Wipe, but the Scheduler will allow you to define a specific time for wiping to be launched or if wiping will be triggered by a special event. These wiping events are efficient measure against people spying on you (e.g. those who want to read your SMS messages or email). Or, which can be a lot more important and critical for your company or your business, it will protect your data from being accessed by any third party - should the mobile device get lost or stolen. The following “occurrence” options will allow you to configure wipe scheduler to protect your private data:

- 1) **Time-based - Hourly, Daily, Weekly, Monthly or Yearly.** SecuWipe can wipe selected areas on specified time or in specific hours of the day, week, on a specific month of the year etc.
- 2) Upon receiving **SMS** containing user defined password or pass-phrase.
- 3) When **untrusted SIM** is inserted into the device SIM slot. It can even be configured to wipe data if no SIM is discovered in the SIM slot, or the GSM function is turned off.
NB: These special events shall be used with care. Please, use this setting with care if your device is automatically turning off GSM mode on low battery OR if you intend to use Airplane mode. Please, also make sure you remember that you have enabled this option before changing SIM cards.
- 4) **Upon Soft Reset.**

For example, you can configure SecuWipe to wipe free space on your device and its media card every Sunday and use U.S. DoD 5220.22-M (E) wiping standard for this. Or you can configure SecuWipe to wipe all SMS messages in case a specific SMS is received or, for example, every second hour.

You can start Wipe Scheduler from SecuWipe main window. Wipe Scheduler window looks like follows:



In this example, we have 3 tasks, where 2 are set to run automatically, while the third one is inactive (see if the checkbox is active or not). You may create as many tasks as you wish by tapping Menu – New task.



The following window will appear:

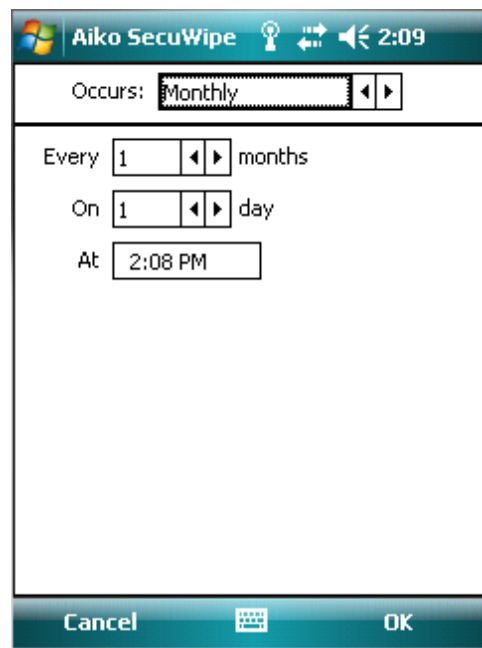
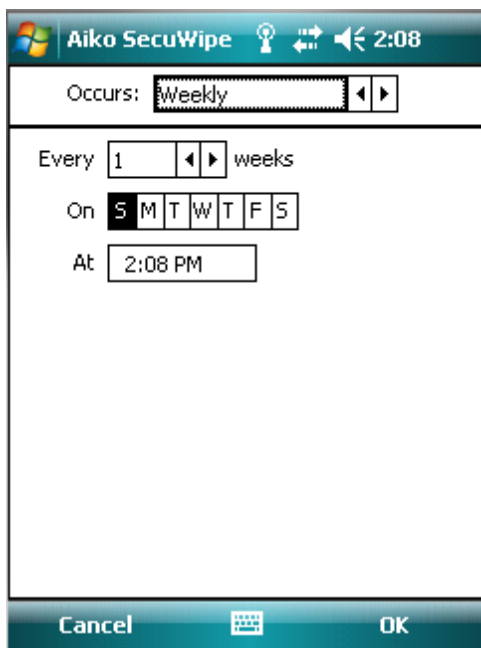
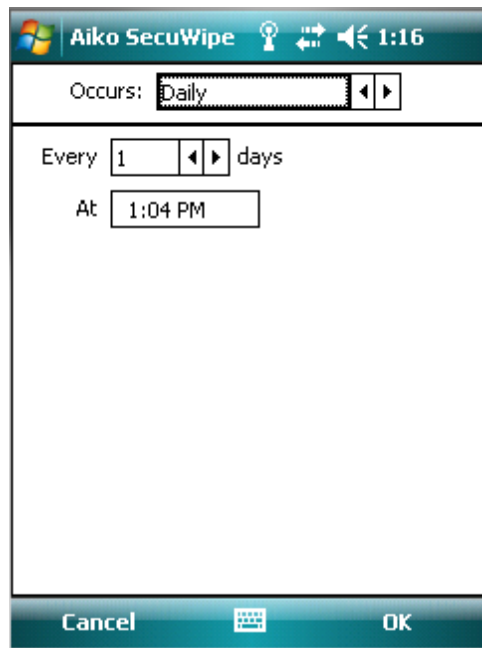
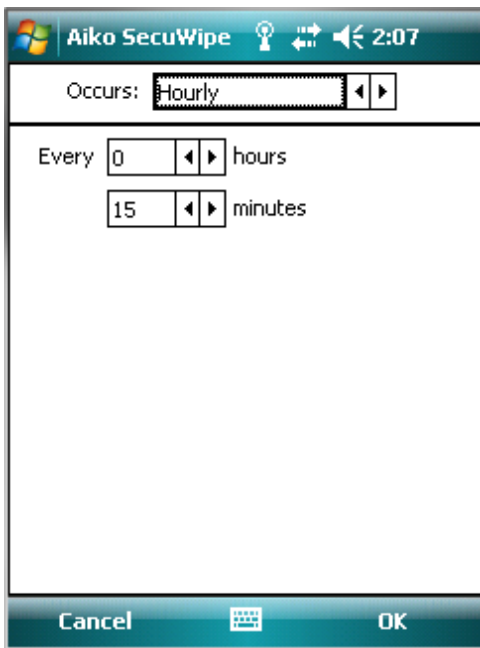
To configure the task, do the following:

1. Type in the Subject of your task
2. Select the Enabled status
3. Define the Objects to be wiped. The Objects may include free space, or SMS, or Internet history, or all data on the device – the Objects you can select are the same you can select during Custom Wipe (see [Custom Wipe for more information](#)) – so you have a great level of flexibility here as well.
4. Select Wiping method
5. Select Start and End date for the wipe task.
6. Select Occurrence – it is here that you define which event will cause the task to run – will it be time based or it will depend on other factors – be it a special SMS with a password, unknown SIM or Soft Reset.

Back to: Contents

Time-based Schedule

With SecuWipe you can wipe your data Hourly, Daily, Weekly, Monthly or Yearly.



Upon Soft Reset

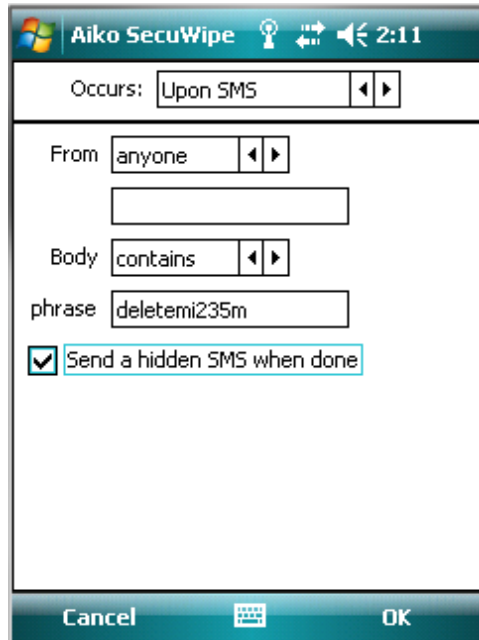
You can use this to launch wiping of the selected objects after you press the soft reset button on your device. This may be useful as a quick solution to wipe all your SMS messages or Internet History or any other specific areas.

NB: Please, make sure you understand that you may lose your data if an accidental soft reset occurs.

Upon SMS

This option is intended to protect your device in the following two cases:

1. You have accidentally left your device at your desk with the information that shall be kept private, but you know that someone else is likely to read the data there. You may then send an SMS from any other phone to wipe the data that could possibly compromise you.
2. In case of the device theft or loss – you may send an SMS to it to wipe it all clean.



The SMS can be received from “anyone” or from a specific number, and the body of this SMS may contain or “be equal to” the passphrase you specify. Once the SMS with this passphrase is received, the wiping of the selected objects will start. You may also get a hidden SMS notification once the wiping process is complete. This SMS will not be stored in the Sent messages.

Back to: Contents

Upon SIM

This is the most efficient, but the most dangerous event. If used wisely, it can ensure confidential data will never get into wrong hands, however, it may also destroy your data if you forget that you have enabled it.

NB: These special events shall be used with care. Please, use this setting with care if your device is automatically turning off GSM mode on low battery OR if you intend to use Airplane mode.

The following events can be enabled:

1) No SIM or Phone off

With this option enabled the selected objects will be wiped if ANY of the following occurs:

- SecuWipe does not “see” the SIM card in the SIM slot
- SecuWipe detects that the phone function of the device is turned off.

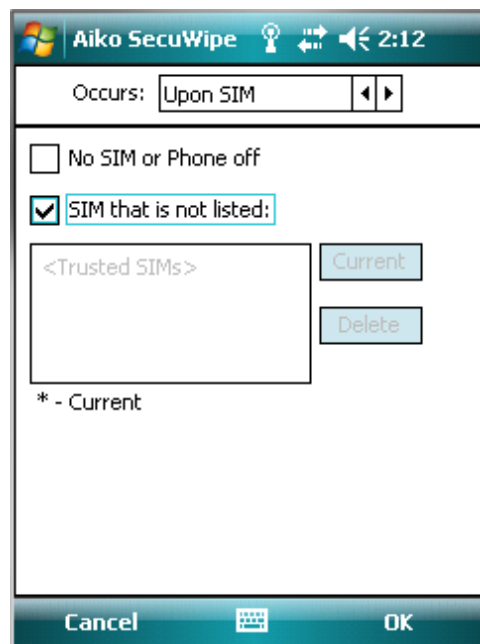
This would be useful in case of the phone theft, when the thief would immediately turn off the phone and remove SIM card. SecuWipe will discover that the SIM was removed and will start

wiping.

2) SIM that is not listed

SecuWipe will wipe selected objects if it discovers the SIM with the unknown ID. You may add as many SIM cards to the trusted list as you wish. To do it, insert the SIM card, and tap Current. The SIM card ID will be added to the trusted SIM cards list.

NB: The number of the SIM card is usually printed on the SIM card itself (directly on the SIM module) - this can be useful when verifying if the SIM is listed in the trusted SIM list or not. However, we have intentionally disabled the ability to enter the SIM number manually. Sometimes the SIM number is printed without the last digit or with an extra digit, that's why it is a lot safer to let SecuWipe read the SIM card number and add it to the trusted SIM list.



Back to: Contents

Settings



Enable System Tray Icon

By default, the system tray icon is enabled. You will find the SecuWipe icon in the lower right corner of your screen. By selecting it, you are able to:

- Wipe file
- Wipe folder
- Wipe free space
- Run Custom Wipe
- Open SecuWipe window for advanced operations
- Exit SecuWipe

Enable Exit Confirmation

With this option enabled you will be able to cancel SecuWipe exit should you accidentally close it.

Minimize to Tray on Close

This is default behavior of the close button of any program in Windows Mobile. However, if you would like to close SecuWipe and close it permanently, then you will need to disable this option.

Check for Updates

You can allow SecuWipe to check for updates if Internet connection is available. Set **Check for updates** to allow the software checking for updates.

Note: no information is being sent to Aiko Solutions or any other party when your software checks for updates.

Autorun at Startup

With this feature enabled, the SecuWipe software will be automatically launched in minimized state after your device is soft reset.

Enable Error Logging

If you experience any unusual behavior, or there are any problems with your installation of SecuWipe, please, select the Enable error logging from the Settings menu. Try to work with SecuWipe to reproduce the problem. After you reproduce the error, please, go to the root folder of your PDA, and find the following files

- a_swmanager.log

Attach this file along with the problem description to the email you send to our support team at support@aikosolutions.com

Warning: error logging seriously slows down SecuWipe software, therefore, do not forget to disable it during normal use!

Exiting SecuWipe

Once started, SecuWipe normally runs in the background, allowing you to wipe file at any time. However, if you want to permanently close the software, you can do it by:

- Going to Menu-> Wipe->Exit
- Selecting SecuWipe icon in system tray and selecting Exit from menu

Back to: Contents

Command line support

Using command line you can create special .lnk files to customize and automate SecuWipe processes - either for automatic and silent wiping, for integration with your own applications or for execution in conjunction with autorun scripts.

The command line syntax is:

```
..\secuwipe.exe [/option][:parameter]
```

You can specify the following options when working with SecuWipe from command line:

/silent – SecuWipe will execute with no warning dialog, no progress bar dialog, no success message. The executable will be remaining in RAM if */unload*-flag is not set

/unload – SecuWipe will be unloaded after it finishes operation. This will close .exe in any case - even if the application returned some kind of error.

/wipe:<folder path> - wipes the specified folder and specific file

/format - it is an additional flag to the command

/wipe:<folderpath> /freespace – the selected folder will be wiped, then the remaining free space

"/wipe:<folderpath> /freespace /format" – in case the storage card has been selected to be wiped - the card will be formatted before wiping

/minimize - minimizes SecuWipe automatically on launch, hides the main window

/freespace

- erases the free space on the device pointed to by the */wipe* switch (must be used with the */wipe* switch)
- Can be also used as a standalone parameter to wipe particular memory, e.g.
/freespace:"Storage Card" ;
- Can be an additional flag to */wipe* - to wipe the remaining space, e.g. */wipe:\doc.txt /freespace*

Selecting Wipe methods:

/level:1|2|3|4|5|6 – is an additional flag to */wipe* and */freespace*, e.g. */wipe:\file.bin /level:2*

Level 1 – zero filling

Level 2 - U.S. DoD 5220.22-M (C)

Level 3 - U.S. DoD 5220.22-M (E)

Level 4 - U.S. DoD 5220.22-M (ECE)

Level 5 - Bruce Schneier's algorithm

Level 6 - Peter Gutmann's algorithm

Back to: Contents

Command Line Usage Examples

1. Wipe file "*\My Documents\Note1.pwi*" without freespace and wiping level "DoD 5220.22-M (E)":

SecuWipe.exe /wipe:"My Documents\Note1.pwi"

2. Wipe file "*\My Documents\Note1.pwi*" without freespace wiping and wiping level "DoD 5220.22-M (ECE)":

SecuWipe.exe /wipe:"My Documents\Note1.pwi" /level:4

3. Wipe file "*\My Documents\Note1.pwi*" with freespace and wiping level "DoD 5220.22-M (C)":

SecuWipe.exe /wipe:"My Documents\Note1.pwi" /freespace /level:2

4. Wipe "*\Temp*" folder without freespace and wiping level "Peter Gutmann's algorithm":

SecuWipe.exe /wipe:\Temp /level:6

5. Wipe "*\Temp*" folder without freespace wiping and level "Bruce Schneier's algorithm":

SecuWipe.exe /wipe:\Temp /level:5

6. Wipe "*\Temp*" folder with freespace and "Zero-filling":

SecuWipe.exe /wipe:\Temp /freespace /level:1

7. Wipe main memory freespace and "DoD 5220.22-M (E)":

SecuWipe.exe /freespace /level:3

8. "Storage Card" freespace wiping with "DoD 5220.22-M (C)":

SecuWipe.exe /freespace:"Storage Card" /level:2

9. "Storage Card" content wiping with "DoD 5220.22-M (C)":

SecuWipe.exe /wipe:"Storage Card" /level:2

10. "Storage Card" complete wiping (both data and free space) with "DoD 5220.22-M (E)":

SecuWipe.exe /wipe:"Storage Card" /freespace

11. "Storage Card" complete wiping (both data and free space) with "DoD 5220.22-M (E)" but with formatting before wiping:

SecuWipe.exe /wipe:"Storage Card" /freespace /format

Back to: [Contents](#)

Performance - Wipe Speeds

The time it takes for SecuWipe to complete a wipe is not dependent on what type of data exists on the device or memory card. For example, an empty memory card will wipe at the same speed as a card completely full of data. A pass of writing random characters will take more time as each character must be individually generated.

Platform: Windows Mobile 6.0 Professional

CPU: SC32442-400MHz

Memory card: MicroSD Kingston 2GB

File/folder size	Zeroing-out 1 pass	U.S. DoD 5220.22-M (C)- 1 pass	U.S. DoD 5220.22-M (E) – 3 passes	U.S. DoD 5220.22-M (ECE) – 7 passes	Bruce Schneier's algorithm - 7 passes	Peter Gutmann's algorithm - 35 passes
100 Mb	00:00:35	00:03:11	00:14:47	00:43:15	00:44:26	03:37:52
1 Gb	00:07:02	00:42:48	03:20:26	07:04:15	07:18:26	35:34:19
2 Gb	00:10:16	01:02:00	04:50:51	14:09:16	14:31:13	70:32:21

Note: here 1 Mb is equal to 1 000 000 bytes, 1 Gb is equal to 1 000 000 000 bytes

Back to: [Contents](#)

Recommended Procedures

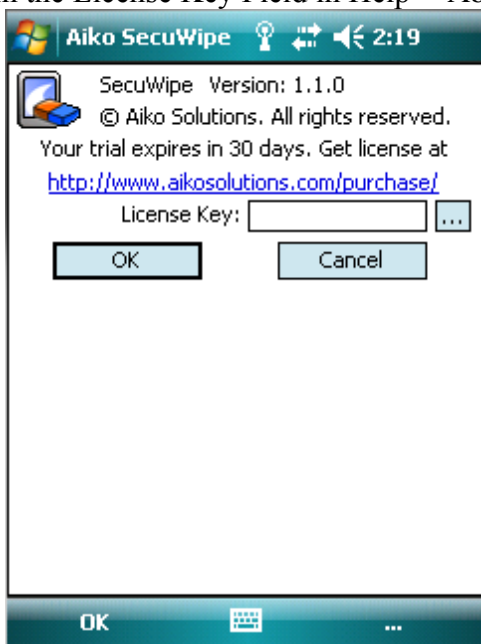
If you are selling or donating your Windows phone or Pocket PC, we recommend the following procedure to eliminate all traces of proprietary information:

1. Run Custom Wipe from SecuWipe menu and select all email, contacts, tasks and other databases; select “wipe free space”, select “wipe storage cards”. Select wiping algorithm and continue to wipe. U.S. DoD 5220.22-M (E) – 3 passes is what we recommend for wiping sensitive information.
2. Hard reset the device.
3. Perform “Wipe Free Space” again.

How to Register

The unregistered version of SecuWipe can be used for 30 days. If you like the application, please register your copy. You can order SecuWipe for \$39.95.

To get a license for your copy of SecuWipe, please, visit www.aikosolutions.com/purchase/ and select the appropriate license scheme. Academic and Research institutions worldwide are eligible for special highly discounted licensing scheme. After you purchase the license, you will then get an email with the registration key. Please, enter it in the License Key Field in Help-> About dialog.



Back to: Contents

Contacts

For further information about Aiko Solutions or any of our products, please visit www.aikosolutions.com or contact us at:

For sales: sales@aikosolutions.com

For technical questions: support@aikosolutions.com

For other questions: info@aikosolutions.com

Back to: Contents

© 2008-2010 Aiko Solutions Ltd